BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PCT/EP 97/03113

BUNDESREPUBLIK DEUTSCHLAND

09/202536

Bescheinigung

Herr Dr. Erland W i t t k ö t t e r in Konstanz/ Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Vorrichtung und Verfahren zum geschützten Übertragen und Darstellen elektronisch publizierter Dokumente"

am 14. Juni 1996 beim Deutschen Patentamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patentamt vorläufig die Symbole G 06 F und H 04 L der Internationalen Patentklassifikation erhalten.

München, den 3. Juli 1997
Der Präsident des Deutschen Patentamts
Im Auftrag

Aktenzeichen: 196 23 868.4

Agurks

HIEBSCH PEEGE

PATENTANWÄLTE
EUROPEAN PATENT ATTORNEYS

Patentanwälte Hiebsch e.a., Postfach 464, D-78204 Singen

Dipl.-Ing. Gerhard F. Hiebsch
Dipl.-Ing. Klaus Peege
Dipl.-Ing. Niels Behrmann M.B.A. (NY)

D-78224 Singen/Germany
Heinrich-Weber-Platz 1

Telephon/e (07731) 4 30 55
Telefax (07731) 4 20 99
Telex 793 850 hpsi
eMail Bodenseepatent®@t-online.de

Unser Zeichen: ***W189DE1***
Our file: ***B/mü***

1) ***Prioritätsnummer / Priority Application Number:***

(32) ***Prioritätstag / Priority Date:***

(33) ***Prioritätsland / Priority Country:***

(54) ***Titel / Title:*** ***Vorrichtung und Verfahren zum geschützten Übertragen und Darstellen elektronisch publizierter Dokumente.***

(71) ***Anmelder/in / Applicant:*** ***Dr. Erland Wittkötter***
Abendbergweg 7
D-78465 Konstanz

(73) ***Erfinder / Inventor:*** ***-wird / werden nachbenannt-***

(74) ***Vertreter / Agent:*** ***Dipl.-Ing. Gerhard F. Hiebsch***
und Kollegen
-Patentanwälte-
Heinrich-Weber-Platz 1
D-78224 Singen

Vorrichtung und Verfahren zum geschützten Übertragen und Darstellen elektronisch publizierter Dokumente

Die vorliegende Erfindung betrifft eine Vorrichtung zum Schützen elektronisch publizierter Dokumente nach dem Oberbegriff des Patentanspruchs 1 sowie ein Verfahren nach dem Oberbegriff des Patentanspruchs 9.

Durch die zunehmende Verbreitung elektronischer Datennetze und unabhängiger Datenträger (z.B. CD-ROM), den sich ständig erweiternden Benutzerkreis und die Verbesserung der Übertragungs- und Zugangstechnologie für Online-Dienstleistungen ergeben sich auch neue Möglichkeiten, elektronische Dokumente (bzw. Medien) über solche Datennetze -- beispielsweise das Internet -- anzubieten und zu publizieren; zu diesen Produkten gehören neben Texten und Bildern auch Audio- oder Videomedien.

Mit der Schaffung der technologischen Rahmenbedingungen für eine derartige, elektronische Publikation entsteht die technische Herausforderung, derartige Medien vor unberechtigtem Zugriff bzw. illegalem Kopieren zu schützen, so daß das Copyright des Anbieters wirksam bewahrt werden kann: Durch den digitalen Charakter der elektronisch publizierten Information könnte ein (auch unberechtigtes) Kopieren ohne Qualitätsverlust erfolgen; daher ist die Frage des Schutzes solcher elektronischen Publikationen existentielle und fundamentale Schlüsselfrage für die öffentliche Freigabe von (herkömmlichen) Video-, Audio- und Printmedien in elektronischer Form.

Aus der EP 0 665 486 A2 ist ein Verfahren bekannt, mit welchem elektronisch publizierte Medien geschützt werden können, um den vorstehend umrissenen Zweck zu erreichen.

Bei diesem Verfahren aus dem Stand der Technik handelt es sich um ein i. w. kryptographisches Verfahren, bei welchem über ein Netzwerk ein (elektronisches) Dokument übertragen wird, das anschließend auf dem lokalen Rechner zu entschlüsseln ist. Dabei beruht die Möglichkeit des lokalen Benutzers zur Entschlüsselung auf einer über das Netzwerk erfolgenden Authentisierung des Benutzers und einer entsprechenden, individuellen Codierung. Darüber hinaus wird das Dokument elektronisch so eindeutig gekennzeichnet, daß eine Identifikation einer illegalen Kopie auf den ursprünglichen Nutzer zurückgeführt werden kann -- also zumindest eine rechtliche Durchsetzung der Ansprüche nach dem Auftreten eines illegalen Zugriffs bzw. einer unbefugten Kopie möglich ist.

Dieses Verfahren nach dem Stand der Technik ist allerdings in mehrfacher Hinsicht nachteilig: So ist der Übertragungs- und Rechenaufwand allein schon deswegen beträchtlich, als für jeden identifizierten und authentisierten Benutzer eine spezifische Fassung des vollständigen Dokuments über das Netz übertragen werden muß; neben dem Verschlüsselungsaufwand für das gesamte Dokument findet daher der Transport eines -- gerade bei multimedialen Dokumenten -- nicht unbeträchtlichen Datenvolumens statt. Zwar ist davon auszugehen, daß zukünftig durch leistungsfähige Rechenanlagen dieses Verfahren auch für eine Vielzahl von (möglicherweise gleichzeitig) zugreifenden Benutzern in akzeptabler Zugriffszeit funktioniert; allerdings bleibt dann nach wie vor das Problem, daß möglicherweise die Netzkapazitäten zum Übertragen der Datenmenge des vollständigen Dokuments -- gerade für Echtzeitbetrieb -- nicht immer ausreichen.

Aufgabe der vorliegenden Erfindung ist es daher, eine gattungsgemäße Vorrichtung bzw. ein Verfahren zum geschützten Übertragen und Darstellen von elektronisch publizierten Dokumenten zu schaffen, welches diese Nachteile aus dem Stand der Technik überwindet und

insbesondere ein einfacheres, flexibleres und sicheres elektronisches Publizieren der Dokumente auch über ein Datennetz mit langsamerer Übertragungsgeschwindigkeit und/oder geringerer Übertragungskapazität ohne Qualitätseinbußen ermöglicht. Darüber hinaus sollten die erfindungsgemäß zu publizierenden Dokumente potentiell einer unbegrenzten Anzahl von Nutzern zugänglich zu machen sein (ohne daß, wie beim vorzitierten Stand der Technik, jeweils individuelle komplette Verschlüsselungen für einen jeweiligen Nutzer -- zeit- und rechenaufwendig -- erfolgen müssen).

Die Aufgabe wird durch die Vorrichtung nach dem Patentanspruch 1 sowie das Verfahren nach dem Patentanspruch 9 gelöst.

Vorteilhaft gestattet dabei das lokale Speichern des elektronisch publizierten Dokuments, allerdings in einer für den Benutzer ohne die zusätzlichen, externen Daten unbrauchbaren Weise, das unverschlüsselte, identische Verteilen einer theoretisch unbegrenzten Anzahl identischer Dokumente, ohne daß durch Kopieraktion od. dgl. ein Eingriff in die Rechte des Anbieters erfolgen kann. Andererseits findet aber über das Datennetz ein Austausch der zusätzlichen Daten statt, mit welchen dann durch die Verknüpfungseinrichtung die lokal abgelegten Dokumentdaten für den Benutzer in eine brauchbare und sinnvolle Form gebracht werden können.

Diesbezüglich ist erfindungsgemäß unter "Datenübertragungsnetz" jedes elektronische Netzwerk zu verstehen, mit welchem über den lokalen Bereich hinaus Daten zwischen Computern übertragen bzw. ausgetauscht werden können.

Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen beschrieben.

So werden besonders bevorzugt die elektronisch publizierten Dokumente in der lokalen Datenspeichereinrichtung in einer nicht-linearen Form gespeichert, wobei im Zusammenhang mit der vorliegenden Erfindung der Begriff "linear" wie folgt verstanden werden soll: Lineare Medien, also Medien, die als lineare Kette von Seiten, Bildern oder anderen Informationsträgern aufgefaßt werden können, bestehen aus einer Anzahl von Inhalten bzw. Inhaltsträgern (bei Druckwerken also beispielsweise Seiten), die über eine Struktur (also Seitenzahlen bzw. die physische Anordnung in einem - gedruckten - Buch) miteinander verbunden und in eine sinnvolle Reihenfolge gebracht werden. Mit Hilfe der Strukturelemente kann also selbst ein Dokument aus einer Mehrzahl von nicht-linearen Inhaltsträgern, die in einer beliebigen Reihenfolge abgelegt und somit als Gesamtdokument für einen Benutzer nicht brauchbar sind, in eine lineare, nutzbare Struktur gebracht werden.

Insoweit bewirken die zusätzlichen Daten also eine gerichtete bzw. bidirektionale Verbindung (Link) zwischen zwei getrennten Teilen eines oder mehrerer Dokumente. Linearität eines Dokuments bedeutet somit die einfach skalierte Reihenfolge bzw. Anordnung der einzelnen Informationsträger, während Nicht-Linearität im vorliegenden Sinne die Abweichung von der linearen Anordnung (mindestens von Teilen) des Mediums ist.

Besonders geeignet kann als lokale Datenspeichereinrichtung ein Permanentspeicher -- beispielsweise als optisch lesbare CD -- benutzt werden, welcher mit geringem Aufwand in großen Stückzahlen herstellbar ist. Auf dieser CD könnten dann -- nicht-linear -- die einzelnen Informationsträger des Dokuments in einer von der natürlichen Dokumentenreihenfolge abweichenden Anordnung gespeichert sein, ohne daß die CD zusätzlich Daten bzw. Informationen über das Anordnen der Informationsträger in die brauchbare Reihenfolge enthält. Vielmehr würden diese zusätzlichen

Informationen, die erst die Linearität des Dokuments herbeiführen, extern über das Netz herangeführt.

Alternativ ist es im Rahmen der vorliegenden Erfindung möglich, eine Nicht-Linearität in der Weise in der lokalen Datenspeichereinrichtung zu realisieren, als das dort gespeicherte Dokument eine Anzahl von Datenlücken aufweist, ohne deren Dateninhalt das Dokument für den Benutzer unbrauchbar ist. Diese Datenlücken ausfüllenden Daten können nunmehr entweder als zusätzliche Daten aus der externen Datenquelle über das Netz herbeigeführt werden, oder aber auch die Lückendaten können -- allerdings getrennt von dem Restdokument -- lokal gespeichert sein, und als externe Daten würden lediglich wiederum Verbindungs- bzw. Indexdaten zum Verknüpfen der Lücken und der zugehörigen Lückendaten herbeigeführt.

Gemäß einer bevorzugten Weiterbildung der Erfindung, die insoweit als beste Ausführungsform der Erfindung anzusehen ist, weist die erfindungsgemäße Vorrichtung zusätzlich eine Verschlüsselungsvorrichtung auf, mit welcher die über das Datennetz übertragenen, zusätzlichen Arten verschlüsselt werden, um auf lokaler Seite die Sicherheit des brauchbaren Zugriffs auf die Dokumente weiter zu erhöhen: Bevorzugt im Wege einer der Verschlüsselung zugrundeliegenden Schlüsselvereinbarung zwischen der externen Datenquelle und dem lokalen Computersytem findet dann ein vor Drittzugriff geschützter Austausch der zusätzlichen Daten -- also beispielsweise der Reihenfolge- oder Lückendaten -- statt, und erst nach lokaler Entschlüsselung dieser zusätzlichen Daten werden diese durch die Verknüpfungseinrichtung in brauchbare Dokumente aufbereitbar.

Weiter bevorzugt ist ein Identifikations- oder ein Abrechnungsmodul vorgesehen, mit welchem Informationen des Benutzers, also beispielsweise zum Zweck der Gebührenerfassung und -abrechnung, erfaßt und weiterverarbeitet werden können. (In Abgrenzung zum

eingangs zitierten, gattungsbildenden Stand der Technik ist lediglich zu diesem Zweck eine Identifikation des externen Benutzers durch die Datenquelle notwendig). Es kann zwischen dem Host und dem Benutzer eine elektronische Währung in Form von zufälligen, nur einmal verwendbaren Zeichenfolgen ("one-time pads") definiert werden, die dem Benutzer erlaubt, seine Rechte am Lesen der Dokumente weiterzugeben.

Schließlich sorgt erfindungsgemäß ein Steuermodul für den reibungslosen Datenaustausch mit der externen Datenquelle.

Durch die Erfindung kann somit sichergestellt werden, daß ein unbefugtes Kopieren und Verbreiten der Dokumente unmöglich ist; gleichzeitig ist es aber möglich, auf lokaler Benutzungsseite das beliebige Kopieren bzw. Weitergeben der lokal gespeicherten Dokumentdaten nicht nur zu dulden, sondern ggf. sogar zu fördern, um somit einen möglichst großen, potentiellen Nutzerkreis für die elektronisch publizierten Daten zu erreichen. Gleichzeitig tritt die vorteilhafte Wirkung ein, daß erfindungsgemäß das über das Netz von der externen Datenquelle zu übertragene Datenvolumen minimiert und nur auf die erfindungsgemäß zusätzlichen Daten beschränkt ist. Darüber hinaus ließe sich durch eine Komprimierung der externen, zusätzlichen Daten (bzw. auch der lokal gespeicherten Dokumentdaten) eine weitere Optimierung der Datenübertragung in mengenmäßiger und zeitlicher Sicht erreichen.

Gemäß weiterer, bevorzugter Weiterbildungen der Erfindung wird das erfindungsgemäße Verfahren realisiert, in dem Plattform-unabhängig (d. h. unabhängig von verwendeten Hardware- oder Softwaresystemumgebungen) der erfindungsgemäße Ablauf realisiert wird und zusätzlich Routinen zur Integritätsprüfung einbezogen werden, mit welchen festgestellt werden kann, ob der externe Benutzer ordnungsgemäß zugreift, oder aber unzulässige Zugriffsversuche unternommen werden.

Erfindungsgemäß kann daher mit dem Verfahren bzw. der Vorrichtung realisiert werden, daß der Benutzer nur genau definierte Prozesse auf die Dokumente anwenden darf -- beispielsweise kann das Ausdrucken erlaubt werden, dieses aber auch durch geeignete Einrichtung (und ggf. externe Kontrolle über das Netz) ausgeschlossen sein. Darüber hinaus wird erfindungsgemäß sichergestellt, daß ein Abspeichern der lokal generierten, benutzbaren Dokumentinformation nicht möglich ist.

Auch kann weiterbildungsgemäß ein elektronisch publiziertes Dokument mit einem (elektronischen) Verfallsdatum in absoluter oder relativer Form versehen werden, wobei auch der beabsichtigte Zweck des Verfalldatums nicht durch manipulative Maßnahmen am lokalen Computersystem vereitelbar ist, da ein entsprechendes, mit einem Dokument verknüpftes Datum stets abhängig vom extern, über das Netz übertragenen Datum ist. Auf entsprechende Weise können Aktualisierungen und dgl. des Dokuments erfolgen.

Weitere Vorteile, Merkmale und Einzelheiten der Erfindung ergeben sich aus der nachfolgenden Beschreibung von Ausführungsbeispielen anhand der Zeichnung; diese zeigt in

Fig. 1: ein schematisches Funktionsschaltbild der erfindungsgemäßen Vorrichtung zum Schützen elektronisch publizierter Dokumente gemäß einer ersten, bevorzugten Ausführungsform mit zusätzlich eingezeichneten, möglichen Weiterbildungen;

Fig. 2: ein Verfahrensablaufdiagramm des erfindungsgemäßen Verfahrens zum Schützen elektronisch publizierter Dokumente gemäß einer bevorzugten Ausführungsform;

Fig. 3: ein Verfahrensablaufdiagramm eines im Rahmen des Verfahrens gemäß Fig. 2 durchgeführten Aktualisierungs- und Testverfahrens und

Fig. 4: eine schematische Darstellung eines elektronisch publizierten Dokumentes im geschützten, nicht-linearen Zustand (a) bzw. im erfindungsgemäß behandelten, durch Hinzufügen von Verbindungsdaten linearisierten Zustand (b).

Ein elektronisches Netzwerk 10 -- welches ein beliebiges privates oder öffentliches Netzwerk zur Verbindung einer Mehrzahl von elektronischen Datenverarbeitungsanlagen zum Zweck des Datenaustausches zwischen diesen sein kann, und im vorliegenden Ausführungsbeispiel das öffentlich zugängliche Internet ist -- stellt eine Verbindung zwischen einem

externen Host-System, begrenzt durch die Linie 12 in Fig. 1, und einem aus einer Mehrzahl lokaler Computer, begrenzt durch die rechte Linie 14, her.

Während das Host-System 12 von dem Anbieter und Distributor elektronisch über das Netz 10 anzubietender Nutzerdaten -- im dargestellten Beispiel Grafikdaten -- betrieben wird, ist der lokale Computer zum Abrufen und Darstellen der durch den Betreiber des Host-Systems 12 angebotenen Nutzerdaten am Aufstellungsort des lokalen Computers 14 vorgesehen. Zu diesem Zweck weist der lokale Computer 14 eine von der gestrichelten Linie umrandete Verarbeitungseinheit 16 auf, die einerseits mit einem Dokumentspeicher 18 und anderseits mit einer Ausgabeeinheit 20 sowie einer Eingabeeinheit 22 verbunden ist und mit diesen Peripheriegeräten zusammenwirkt. Darüber hinaus ist die Verarbeitungseinheit 16 zum Zusammenwirken mit dem Netz 10 eingerichtet.

Der Dokumentspeicher 18 ist im vorliegenden Ausführungsbeispiel als lokaler, unmittelbar mit der Verarbeitungseinheit 16 verbundener Massenspeicher realisiert, der bereits Bestandteile des über das Netz elektronisch zu publizierenden Dokuments enthält. Die Ausgabeeinheit 22 stellt die Verbindung zwischen dem lokalen Computer 14 und dem Benutzer her und wird in Abhängigkeit von dem zu publizierenden Dokument gewählt: Im vorliegenden Fall der Publikation elektronischer Zeichnungen und Grafiken würde die Ausgabeeinheit 20 i.w. aus einem zur Darstellung dieser Grafiken geeigneten Monitor mit zugehöriger Datenaufbereitung bestehen, während in anderen Anwendungsfällen -- etwa der Übertragung von Texten oder zusätzlichem Ton, wie bei audiovisuellen, elektronischen Medien -- zusätzlich oder alternativ eine akustische Ausgabeeinheit, ein Drucker od.dgl. angeschlossen sein kann. Die Eingabeeinheit 22 ist z.B. als Tastatur oder Maus ausgeführt und dient dem Benutzer zur Ablaufsteuerung bzw. zur Eingabe von Kommandos

für den Abruf der erfindungsgemäß elektronisch publizierten Dokumente.

Die zentrale Verarbeitungseinheit 16 weist als Komponente eine Schlüsseleinheit 24 mit zugehörigem Schlüsselspeicher 25, ein Dokumentaufbau- bzw. Konstruktionsmodul 26, ein Dialogsteuermodul 28 sowie einen Zeitgeber 30 auf. In der Fig. nicht gezeigt ist ein Kommunikationsmodul, welches für die Zusammenarbeit mit dem Netz 10 vorgesehen ist.

Demgegebenüber ist im Host-System 12 ein Schlüsselservermodul 32, ein Copyrightservermodul 34, ein Abrechnungsservermodul 36 sowie -- fakultativ und im Rahmen einer bevorzugten Weiterbildung -- ein Dokument- bzw. Updateservermodul 38 vorgesehen.

Die Funktion und Wirkungsweise dieser Module wird nachfolgend erläutert, wobei im vorliegenden Ausführungsbeispiel die Funktionen dieser Module bevorzugt durch geeignet programmierte Software im Host-System 12 bzw. im lokalen Computer 14 realisiert sind; jedoch, wie dem Fachmann ohne weiteres klar ist, könnten diese Module jeweils auch als diskrete Hardwaremodule mit konventioneller, elektronischer Schaltungstechnologie realisiert sein, die in der angegebenen, prinzipiellen Weise und i.ü. in der dem einschlägigen Durchschnittsfachmann geläufigen Weise verschaltet ist. Der Begriffsbestandteil "Server" deutet auf die Anordnung des betreffenden Moduls im Host-System hin.

Aufgabe und Funktion der Schlüsseleinheit 24 (auch in der Bedeutung von Datensicherungseinheit) ist es, im Datenaustausch mit dem Schlüsselservermodul 32 eine Schlüsselvereinbarung vorzunehmen, also der Schlüsseleinheit 24 einen -- gegen jeglichen Zugriff gesicherten -- eindeutigen und geheimen Schlüssel zur Verfügung zu stellen, mit welchem dann die Schlüsseleinheit eine vom Copyrightservermodul 34 übertragene Reihenfolge- bzw. Lückeninformation entschlüsseln und für die Benutzung durch

das Dokumentaufbaumodul 26 im lokalen Computer bereitstellen kann: Mit Hilfe dieser entschlüsselten Reihenfolge- oder Lückeninformation greift dann das Dokumentaufbaumodul 26 auf den Datenbestand des Dokumentspeichers 18 zu und benutzt die über das Netz empfangene Information des Copyrightservermoduls, um die ungeordneten oder lückenhaften Daten des Dokumentspeichers 18 zu vollständigen Nutzerdaten aufzubereiten, welche dann dem Benutzer über die Ausgabeeinheit 20 bereitgestellt werden.

Während das Dialogsteuermodul 28 das protokollgemäße Zusammenwirken der Funktionsmodule bzw. den korrekten Ablauf des (nachfolgend zu beschreibenden) Verfahrens steuert, dient der Zeitgeber 30 dazu, ggf. periodische Nutzerinformation -- z.B. bewegte Bilder -- in der für den Nutzer geeigneten Weise zusätzlich aufzubereiten.

Auf der Seite des Host-Systems ist schließlich das Abrechnungsservermodul 36 zum korrekten Identifizieren des lokalen Nutzers, Erfassen von dessen Nutzungsumfang an den über das Netz publizierten Dokumenten und letztendlich zum Generieren von entsprechenden Abrechnungsdaten vorgesehen.

Der Dokument-/Updateserver 38 schließlich ist für Einsatzzwecke vorgesehen, bei welchen nicht nur Reihenfolge- oder Lückeninformation, betreffend lokal vorhandene bzw. gespeicherte Dokumentdaten (Dokumentspeicher 18) benutzt werden, sondern ggf. zusätzlich oder statt dessen auch diese Daten -- z.B. in jeweils aktuellster, dem Betreiber Host-seitig vorliegender Form -- über das Netz geliefert (publiziert) werden. Darüber hinaus dient das Modul 38, wie bei der nachfolgenden Beschreibung des erfindungsgemäßen Verfahrens im Detail ausgeführt werden wird, zur Aktualisierung von nutzerseitigen Betriebssystemkomponenten.

Nachfolgend wird anhand der Verfahrensablaufdiagramme der Fig. 2 und 3 der erfindungsgemäße Verfahrensablauf zum Schützen elektronisch publizierter Dokumente beschrieben, wobei auf das in Fig. 1 beschriebene Ausführungsbeispiel Bezug genommen wird.

Zur Verdeutlichung des Verfahrens und zum Beschreiben einer möglichen Form der lokalen Speicherung der Dokumentdaten (im Dokumentspeicher 18) wird ergänzend auf die Darstellung in der Fig. 4 verwiesen, in welcher exemplarisch in der Speicherreihenfolge angeordnete Nutzerdaten sowie deren aufbereitete Form dargestellt ist. Wie in Fig. 4 (a) gezeigt, wird eine elektronische Grafik beispielsweise in acht physisch aufeinanderfolgenden Speicherplätzen im Datenspeicher 18 abgelegt, wobei die Reihenfolge der physischen Speicherplätze 1 bis 8 mit den darin angeordneten Informationseinheiten, wie in Fig. 4 (a) dargestellt, nicht der für einen Benutzer sinnvollen und benutzbaren (brauchbaren) Reihenfolge entspricht -- vielmehr fehlt es an einer sequentiellen Verknüpfung zwischen diesen nichtlinear gespeicherten Dateneinheiten, um zu einer sinnvollen, verständlichen Grafikdatei a-b-c-d-e-f-g-h (Fig. 4 (b)) zu gelangen. Diese Reihenfolgeinformation aber, die im dargestellten Beispiel der Fig. 4 der Anordnung der jeweiligen, physikalischen Speicherplätze in der Reihenfolge 3-2-8-1-5-4-7-6 entsprechen würde, ist im Dokumentspeicher 18 nicht enthalten, sondern wird vom Host-System extern über das Netzwerk 10 übertragen.

Zu Beginn des erfindungsgemäßen Verfahrens wird eine Netzverbindung des Host-Systems 12 über das Netzwerk 10 mit dem lokalen Computer 14 hergestellt; diese Netzverbindung richtet sich nach den für das eingesetzte Netzwerk 10 typischen bzw. notwendigen Protokollen und Bedingungen.

Es folgt im Ablaufdiagramm der Fig. 2 das Durchführen einer (in der Fig. 2 mit A bezeichneten, in Fig. 3 dargestellen) Aktualisierungs- und Testroutine, auf die unten noch im Detail eingegangen wird.

In Schritt S10 wird dann die Integrität des lokalen Systems getestet -- mit Hilfe von Abfragen und Testverfahren also geprüft, ob Mißbrauchsversuche im lokalen Computersystem unternommen werden oder Vorkehrungen dafür getroffen sind -- das lokale Computersystem wird für den nachfolgenden Schlüssel- und Datenaustausch mit dem Host-System initialisiert, und die notwendigen Identifikations- und Abrechnungsdaten mit dem Abrechnungsservermodul 36 werden übertragen.

In der nachfolgenden Schlüsselvereinbarung in Schritt S11 findet dann die Übertragung eines Schlüssels vom (sicheren) Schlüsselservermodul 32 des Host-Systems 12 zum lokalen Computer statt; die Schlüsseleinheit 24 legt diesen Schlüssel im Schlüsselspeicher 25 ab.

In Schritt S12 empfängt der lokale Computer dann das codierte Reihenfolgesignal, also im Beispiel nach Fig. 4 die Zahlenfolge 3-2-8-1-5-4-7-6 in durch den gemäß Schlüsselvereinbarung (Schritt S11) verschlüsselter Form. Der im Schlüsselspeicher 25 abgelegte Schlüssel ermöglicht dann die Entschlüsselung dieses Reihenfolgesignals im Schritt S13 durch die Schlüsseleinheit 24.

Somit steht also für das Konstruktions- bzw. Dokumentaufbaumodul 26 das (entschlüsselte) Reihenfolgesignal bereit, mit welchem das Modul 26 nunmehr auf den Dokumentspeicher 18 zugreifen und die darin gespeicherten Daten gemäß der empfangenen und entschlüsselten Reihenfolge in lesbarer und benutzbarer Weise aufbereiten kann (Schritt S14), so daß dann in Schritt S15 diese aufbereiteten Nutzdaten über die Bildschirm-Ausgabeeinheit 20 und/oder eine Druckereinheit 40 ausgegeben werden können.

In Schritt S16 prüft dann das System, ob entweder eine entsprechende Benutzereingabe bzw. -nachfrage nach weiteren, aufzubereitenden Dokumente besteht, oder aber ob durch die Natur des elektronisch publizierten Dokumentes -- etwa einem Film -- ein kontinuierliches Auslesen von Daten des Datenspeichers 18 zu erfolgen hat. Der durchgezogene Pfeil 42 beschreibt den Verlauf dieser Rückkopplungsschleife, die vor Schritt 14 -- Dokumentaufbau -- wieder ansetzt.
Alternativ könnte allerdings das Verfahren auch zu anderen, früheren Verfahrensstufen rückgekoppelt sein: So wäre beispielsweise in der mit Pfeil 44 gezeigten Weise die Schleife nach Schritt S16 vor Schritt S12 geschlossen, so daß in diesem Fall das lokale System für weitere, lokal aufzubereitende Nutzdaten eine neue, codierte Reihenfolge über das Netz empfangen würde und diese erst vor einer erneuten Durchführung der Aufbereitung und Anzeige in Schritt S14, S15 decodieren würde (S13). Weiter alternativ könnte sogar vor Schritt S11 die Schleife geschlossen werden (Pfeil 46); in diesem Fall würde gar eine neue Schlüsselvereinbarung getroffen und dann die nachfolgende Schleife erneut durchlaufen werden.

Aus obigem ergibt sich, daß insbesondere durch Schleifen mit den Pfeilen 44 bzw. 46 die Datensicherheit der Verbindungsdaten weiter erhöht werden kann.

Unter Bezug auf das Verfahresablaufdiagramm in Fig. 3 wird nunmehr das vorgeschaltete Verfahren gemäß Buchstabe A in Fig. 2 beschrieben, nämlich die gemäß einer bevorzugten Weiterbildung der Erfindung erfolgende Aktualisierung des auf dem lokalen Computer für den Empfang der elektronisch publizierten Dokumente ablaufenden Betriebsprogramme.

Diesem liegt die Überlegung zugrunde, daß derartige Betriebssoftware einerseits die Realisierung des beschriebenen Verfahrens und das Zusammenwirken der beschriebenen Module bestimmen kann, darüber hinaus aber auch Routinen und

Abfragen besitzt, die geeignet sind, um unberechtigte Zugriffe, Manipulationsversuche und dgl. Mißbräuche am lokalen System zu erkennen und zu unterbinden. Im dargestellten Ausführungsbeispiel wird die Programmiersprache Java benutzt, um das beschriebene Verfahren zu realisieren. Darüber hinaus wird ein in Java integriertes Sicherheitsmodell benutzt, um den Schutz der Verschlüsselungsverfahren zu garantieren. Auch ist davon auszugehen, daß die lokale Betriebsprogrammumgebung auf dem lokalen Computer 14 permanent modernisiert und aktualisiert wird, wobei auch Techniken und Prozeduren zur Mißbrauchserkennung kontinuierlich weiterentwickelt werden, so daß sich nicht stets die aktuellste Fassung auf dem jeweiligen lokalen Computer 14 befindet.

Mittels der in Fig. 3 beschriebenen Routine wird es nun möglich, nicht nur über das externe Host-System 12 die lokale Betriebssystemumgebung auf den neuesten Stand zu bringen, sondern auch über diese Aktualisierung extern zu überprüfen, ob der lokale Benutzer in der autorisierten und ordnungsgemäßen Weise das lokale Computersystem 14 betreibt, also Integrität vorliegt.

In Schritt S20 wird das Betriebsprogramm -- im vorliegenden Ausführungsbeispiel unter Java realisiert -- gestartet, woraufhin dann in Schritt S21 das Programm die Verbindung mit dem externen Host-System 12 herstellt. In Schritt S22 findet dann die Abfrage statt, ob -- verglichen mit entsprechenden Identifikationsdaten -- auf dem lokalen System 14 die aktuellste Fassung vorhanden ist; falls dies bejaht wird, kehrt die Routine zum Verfahren gemäß Fig. 2 zurück. Falls allerdings in der Abfrage des Schrittes S22 festgestellt wird, daß die lokal betriebene Fassung nicht auf dem neuesten Stand ist (Nein), wird in Schritt S23 die neueste Fassung gesendet (Schritt S23), gestartet (Schritt S24), und die alte Fassung beendet (S25). Jetzt ist die Voraussetzung geschaffen, im nachfolgenden Schritt S10

(Fig. 2) durch Sicherheitsroutinen die vorbeschriebene Integrität zu überprüfen.

Insbesondere kann auf diese Weise auch dann, wenn ein erfolgreicher Angriff auf den Inhalt eines Dokumentes bekannt wird, dadurch umgehend reagiert werden, daß das Java-Betriebsprogramm entsprechend geändert wird und so eine gleichartige Wiederholung dieser Schutzverletzung ausgeschlossen ist.

Über die vorstehend beschriebenen Verfahrensschritte hinaus ist es nötig, die von einem Benutzer auf die elektronisch publizierten Dokumente anzuwendenden Prozesse genau zu definieren und ggf. zu beschränken. Beispielsweise würde ja ein Ausgeben auf einen Drucker 40 das Kopieren und unautorisierte Vervielfältigen des Dokumentes auf Papier -- allerdings unter Qualitätsverlust -- ermöglichen. Darüber hinaus sollte sichergestellt sein, daß ein (lokales) Zugreifen auf bzw. Abspeichern der ausgegebenen Daten (Schritt S15 bzw. Kontruktions-/Dokumentaufbaumodul 26) nicht möglich ist, so daß auch hier eine Weiterverwendung der Daten, also Mißbrauch, ausgeschlossen wird.

Es kann in der erfindungsgemäß beschriebenen Weise durch elektronische Publikation beispielsweise ein (lokal) abgespeichertes Dokument mit einem durch Konfiguration des Java-Programms erzeugten Verfallsdatum versehen werden, das entweder als absolutes Datum (in Form eines definierten Zeitpunktes) vorgegeben wird, oder es kann ein zeitlich begrenztes Nutzungsrecht (n Stunden) eingeräumt werden; beide Optionen erfordern allerdings in der erfindungsgemäßen Weise einen Online-Zugang des Benutzers.

Gemäß einer Weiterbildung dieses Ansatzes könnte ein Dokument durch sein Verfallsdatum weitere Aktualisierungen anfordern. Besonders geeignet erscheint diese Weiterbildung für Handbücher, Lehrveranstaltungen od.dgl.

Ein anonymisiertes Signal, das aus dem (übertragenen) Dokument herausgesendet wird, könnte dem externen Host-System anzeigen, wie häufig das Dokument gelesen bzw. abgerufen wird; entsprechend wären eine Zeitdauer oder andere, Online-Medien-spezifische Daten erfaßbar, so daß die Möglichkeit besteht, in einfacher und nutzbarer Weise Daten zur Verbesserung des Online-Publikationsangebotes zu gewinnen. Darüber hinaus sind aufbauende Marktuntersuchungen od.dgl. möglich.

Ganz konkret besteht im vorliegenden Verfahren ein sehr wirksamer Kopierschutz gegen auf Compact-Discs (CDs) gespeicherten Medien: Ein Kopieren der als lokaler Dokumentspeicher (Bezugszeichen 18 in Fig. 1 bzw. Fig. 2) dienenden CD würde dann, wenn die Daten auf dieser CD in der gemäß Fig. 4 prinzipiell dargestellten Art abgelegt, mit Lücken versehen oder auf andere Weise in einen unlinearen Zustand versetzt würden, auch nicht verhindert werden können; jedoch wäre das Kopieren für den unbefugten Nutzer sinnlos. Vielmehr müßte mit diesem Ansatz sogar das Kopieren des lokalen Datenspeichers als erwünscht anzusehen sein, da dadurch der potentielle Benutzerkreis erweitert und eine Benutzung ohnehin nur durch Host-Kontakt möglich ist.

Dabei ist das erfindungsgemäße Verfahren nicht auf eine separate Übertragung bzw. Hinzufügung einer Reihenfolge der (nicht linearen) Dokumentdaten, wie in Fig. 4 beschrieben, beschränkt: Vielmehr ist es ergänzend oder alternativ möglich, ein Dokument mit Datenlücken im lokalen Dokumentspeicher abzulegen und die zugehörigen Lückendaten dann entweder extern über das Netz heranzuführen, oder diese ebenfalls lokal zu speichern, um dann lediglich Index- bzw. Verknüpfungsinformationen betreffend die Verbindung zwischen den Lückendaten und dem (Rest-) Dokument extern zu liefern. Diese Lücken können z.B. einzelne Worte eines Textdokuments sein. Auch können gewisse Dateneinheiten mehrfach in einer nutzbaren Reihenfolge dieser Dateneinheiten auftreten.

In der praktischen Realisierung der elektronischen Publikation von Schriftdokumenten ist für die Darstellung der Texte ein Viewer notwendig, der eine eingeschränkte und konfigurierbare Funktionalität besitzt; beispielsweise muß die Ausgabeeinheit eine extern -- d.h. durch Java aktivierbare bzw. deaktivierbare -- Kopier- und Druckoption besitzen. Auch sollte dieser Viewer den nicht autorisierten Zugriff auf den generierten Text verhindern. Während relevante Textformate ASCII, RTF, HTML, Postscript oder PDF sind, kommt es bei der praktischen Realisierung auf Funktionalität, Universalität und Eignung im Zusammenhang mit gängigen Softwarepaketen an. In diesem Zusammenhang sollte PDF bzw. HTML als Grundlage für die Veröffentlichung von Verlags-Dokumenten dienen können.

Ein weiterer Aspekt bei der praktischen Realisierung ist das Löschen aller Seitenangaben innerhalb der Dokumente, um diese für das lokale, sichere Datenspeichern vorzubereiten, wobei dann durch die Reihenfolge-Informationen über das Netz diese notwendigen Verbindungen zur Dokumentnutzung (kontrolliert) wieder hergestellt werden können. Bei sog. Hypertext-Medien kann eine erfindungsgemäße Anwendung bereits durch Entfernen der sog. "Links", der spracheninhärenten Verbindungsstrukturen, erfolgen.

PATENTANSPRÜCHE

1. Vorrichtung zum Schützen elektronisch publizierter Dokumente mit einem lokal über ein Datenübertragungsnetz (10) mit einer externen Datenquelle (12) verbindbaren, lokalen Computersystem (14), das zum Abrufen und Darstellen elektronisch publizierter Dokumente eingerichtet ist,
dadurch gekennzeichnet,
daß das lokale Computersystem (14) eine lokale Datenspeichereinrichtung (18) aufweist, die zum permanenten Speichern von Daten der elektronisch publizierten Dokumente in einer für einen Benutzer nicht brauchbaren Form ausgebildet ist, und das lokale Computersystem (14) Mittel (24) zum Empfangen und Aufbereiten von durch die externe Datenquelle (12) über das Datenübertragungsnetz (10) bereitgestellter, zusätzlicher Daten sowie eine Verknüpfungseinrichtung (26) aufweist, die zum Verknüpfen eines Speicherinhalts der lokalen Datenspeichereinrichtung (18) mit den zusätzlichen Daten und zum Erzeugen des elektronisch publizierten Dokuments in brauchbarer Form daraus eingerichtet ist.

2. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, daß die Datenspeichereinrichtung (18) zum Speichern eines elektronisch publizierten Dokuments in nicht-linearer Weise ausgebildet ist und durch Wirkung der Verknüpfungseinrichtung (26), unter Benutzung der zusätzlichen Daten, das nicht-lineare Dokument in ein für den Benutzer brauchbares, lineares Dokument umsetzbar ist.

3. Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die lokale Datenspeichereinrichtung ein magnetischer und/oder optischer Massenspeicher (18) ist, in welchem Daten des elektronisch publizierten Dokuments permanent in einer Mehrzahl von nicht zusammenhängenden Speicherplätzen gespeichert sind, und die zusätzlichen Daten einen Zusammenhang und/oder eine Reihenfolge der Speicherplätze bezeichnen.

4. Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die lokale Datenspeichereinrichtung ein magnetischer und/oder optischer Massenspeicher (18) ist, Daten des darin gespeicherten, elektronisch publizierten Dokuments Datenlücken aufweisen und die Datenlücken durch die zusätzlichen Daten unmittelbar geschlossen werden können, oder die zusätzlichen Daten Speicherplatzangaben enthalten, die auf separate Speicherplätze der lokalen Datenspeichereinrichtung (18) verweisen, in welchen Lückendaten entsprechend den Datenlücken gespeichert sind.

5. Vorrichtung nach einem der Ansprüche 1 bis 4, gekennzeichnet durch eine mittels eines ersten Moduls (32) der externen Datenquelle sowie eines zweiten Moduls (24) des lokalen Computersystems realisierten Verschlüsselungsvorrichtung, die zum geschützten Übertragen der zusätzlichen Daten von der externen Datenquelle (12) zum lokalen Computersystem (14) eingerichtet ist.

6. Vorrichtung nach einem der Ansprüche 1 bis 5, gekennzeichnet durch ein Identifikations- und/oder Abrechnungsmodul (36), das zum Identifizieren eines Benutzers des lokalen Computersystems und zum Erfassen entsprechender Benutzungs- und/oder Abrechnungsdaten eingerichtet ist.

7. Vorrichtung nach einem der Ansprüche 1 bis 6, gekennzeichnet durch ein im lokalen Computersystem (14) vorgesehenes Steuermodul (28), welches zur Dialog- und Ablaufsteuerung des Datenaustausches mit der externen Datenquelle (12) vorgesehen ist.

8. Vorrichtung nach einem der Ansprüche 1 bis 7, gekennzeichnet durch eine Bedieneinheit (22), die zum Erfassen von Benutzerkommandos und zur Beeinflussung des Betriebs des lokalen Computersystems als Reaktion auf die Benutzerkommandes vorgesehen ist.

9. Verfahren zum geschützten Darstellen elektronisch publizierter Dokumente,
gekennzeichnet durch die Schritte:
   - Abrufen von Dokumentdaten aus einer mit einem lokalen Computersystem (14) verbundenen, lokalen Datenspeichereinrichtung (18), die die Dokumentdaten in einer für einen Benutzer nicht brauchbaren Form speichert,
   - Empfangen (S12) zusätzlicher Daten einer mit dem lokalen Computersystem (14) über ein Datenübertragungsnetz (10) verbundenen, externen Datenquelle und
   - Verknüpfen (S14) der zusätzlichen Daten mit einem Inhalt der lokalen Datenspeichereinrichtung (18) zum Erzeugen von für den Benutzer brauchbaren Daten.

10. Verfahren nach Anspruch 9, gekennzeichnet durch den Schritt:
Ablegen der Benutzerdaten in der lokalen Datenspeichereinrichtung (18) in einer nicht-linearen Form.

11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, daß das Ablegen der Benutzerdaten in einer Reihenfolge erfolgt, die ohne Verknüpfung mit den zusätzlichen Daten keine Darstellung der Benutzerdaten in der brauchbaren Form gestattet.

12. Verfahren nach Anspruch 10, dadurch gekennzeichnet, daß ein lückenhaftes Ablegen der Benutzerdaten dergestalt erfolgt, daß nur durch Verknüpfung mit den zusätzlichen Daten die Lücken geschlossen werden.

13. Verfahren nach einem der Ansprüche 9 bis 12, gekennzeichnet durch die Schritte:
    - Identifizieren des Benutzers in der externen Datenquelle (12) und
    - Austauschen von Benutzer- und/oder Abrechnungsdaten (S10) des Benutzers als Reaktion auf die Identifizierung vor dem Empfangen der zusätzlichen Daten.

14. Verfahren nach einem der Ansprüche 9 bis 13, dadurch gekennzeichnet, daß der Schritt des Empfangens der zusätzlichen Daten die Schritte aufweist:
    - Verschlüsseln der zusätzlichen Daten durch die Datenquelle (12),
    - Übertragen der verschlüsselten, zusätzlichen Daten über das Datenübertragungsnetz (10) und
    - Entschlüsseln der verschlüsselten, zusätzlichen Daten durch das lokale Computersystem (14).

15. Verfahren nach Anspruch 14, gekennzeichnet durch den Schritt:
    Vereinbaren eines Schlüssels (S11) zwischen der externen Datenquelle (12)und dem lokalen Computersystem (14) vor dem Schritt des Verschlüsselns.

16. Verfahren nach einem der Ansprüche 9 bis 15, gekennzeichnet durch das aufeinanderfolgende Abrufen und Darstellen einer Mehrzahl von Dokumenteinheiten, wobei für jede der Dokumenteinheiten ein Satz der zusätzlichen Daten empfangen wird.

17. Verfahren nach einem der Ansprüche 9 bis 16, dadurch gekennzeichnet, daß das Empfangen der zusätzlichen Daten abhängig ist von einer einmaligen und/oder temporären durch Vereinbarung zwischen dem lokalen Computersystem (14) und der externen Datenquelle (12) festgelegten Zugangsberechtigung.

ZUSAMMENFASSUNG

Vorrichtung zum Schützen elektronisch publizierter Dokumente mit einem lokal über ein Datenübertragungsnetz (10) mit einer externen Datenquelle (12) verbindbaren, lokalen Computersystem (14), das zum Abrufen und Darstellen elektronisch publizierter Dokumente eingerichtet ist, wobei das lokale Computersystem (14) eine lokale Datenspeichereinrichtung (18) aufweist, die zum permanenten Speichern von Daten der elektronisch publizierten Dokumente in einer für einen Benutzer nicht brauchbaren Form ausgebildet ist, und das lokale Computersystem (14) Mittel (24) zum Empfangen und Aufbereiten von durch die externe Datenquelle (12) über das Datenübertragungsnetz (10) bereitgestellter, zusätzlicher Daten sowie eine Verknüpfungseinrichtung (26) aufweist, die zum Verknüpfen eines Speicherinhalts der lokalen Datenspeichereinrichtung (18) mit den zusätzlichen Daten und zum Erzeugen des elektronisch publizierten Dokuments in brauchbarer Form daraus eingerichtet ist.

(Fig. 1)

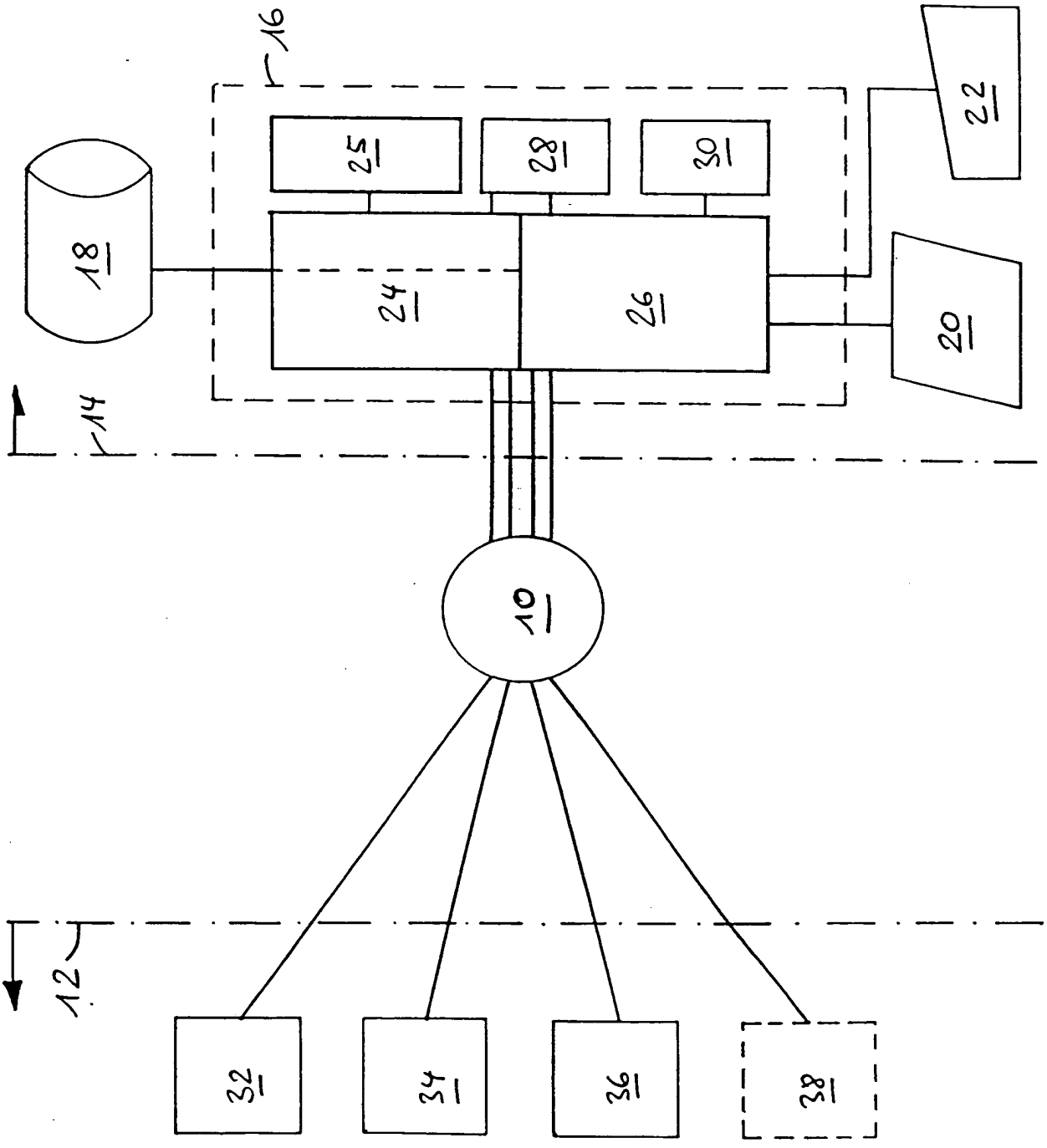


Fig.1

Fig. 2

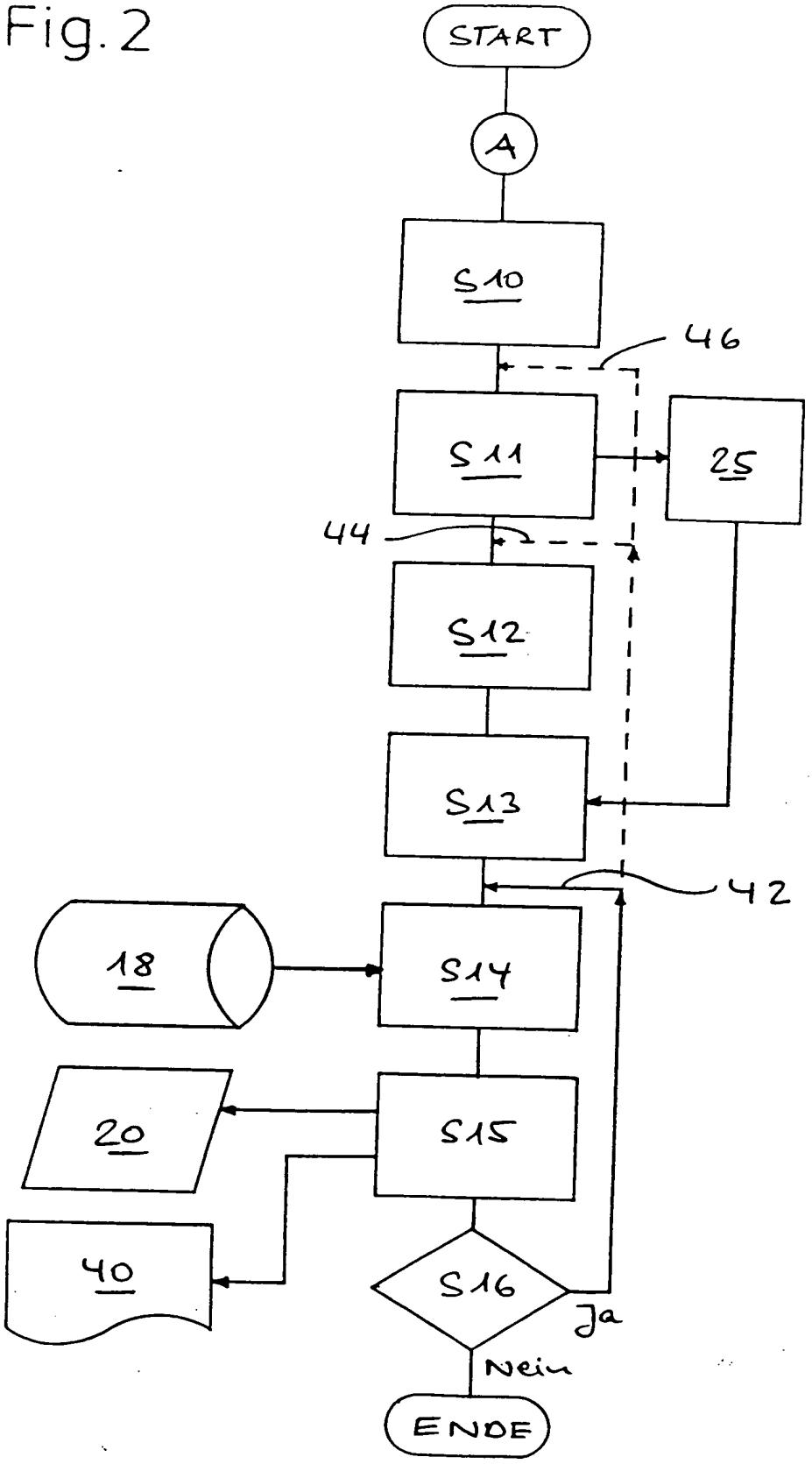

START
A
S10
46
S11
25
44
S12
S13
42
18
S14
20
S15
40
S16
Ja
Nein
ENDE

Fig.4

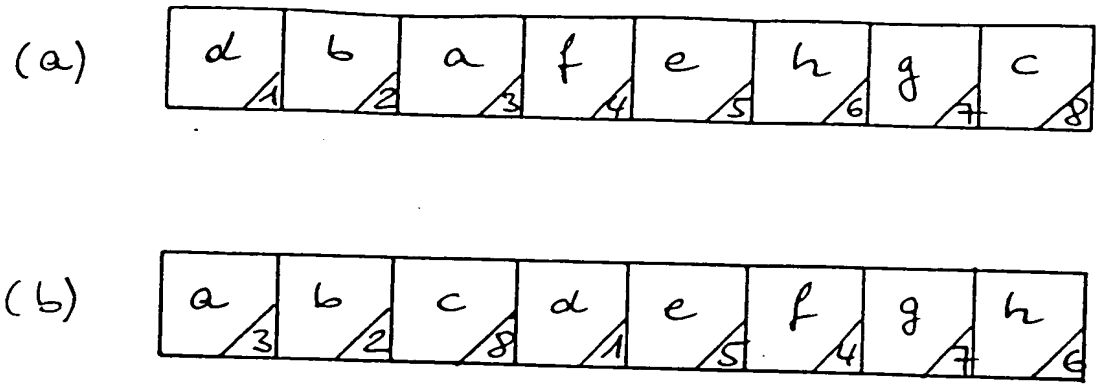
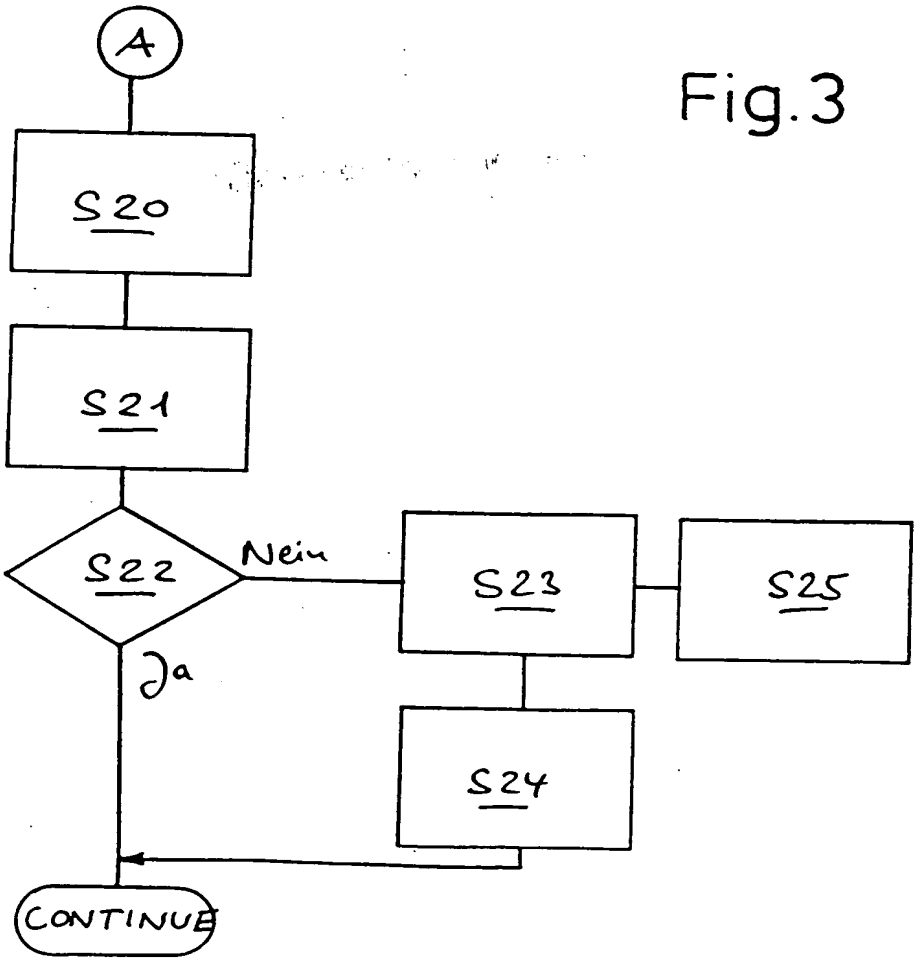

(a)
d b a f e h g c
1 2 3 4 5 6 7 8
(b)
a b c d e f g h
3 2 8 1 5 4 7 6

Fig.3


A
S20
S21
S22
Nein
Ja
S23
S25
S24
CONTINUE